Вариант 6

Зашифрованное сообщение	Шххзалфпл
Ключ, k	7

Вариант 7

Зашифрованное сообщение	Тцлршцйзхрм
Ключ, k	8

Вариант 8

Зашифрованное сообщение	Нултхсфлфхзпг
Ключ, k	3

Вариант 9

Зашифрованное сообщение	Ешчйтчнщнпеынд
Ключ, k	5

Вариант 10

Зашифрованное сообщение	Дпжтфмцр
Ключ, k	4

Атбаш

Шифр Атбаша – это древний шифр, который использовался для замены букв в тексте. В этом шифре каждая буква заменяется на букву, которая находится на том же месте в обратном порядке алфавита.

Таблица 6. Шифр Атбаш

Исходный алфавит

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Алфавит для шифрования

Я Ю Э Ь Ы Ъ Щ Ш Ч Ц Х Ф У Т С Р П О Н М Л К Й И З Ж Ё Е Д Г В Б А

Таблица 7. Пример шифрования

Исходное сообщение	МИРЭА
Зашифрованное сообщение	ТЦОВЯ

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	Лсцэъонцмъм

Вариант 2

Зашифрованное сообщение	Фцюъосъмцфя

Вариант 3

Зашифрованное сообщение	Фоцпмрьоякца

Вариант 4

Зашифрованное сообщение	Жцкорэясцъ

Вариант 5

Зашифрованное сообщение	Цскротяица

Вариант 6

Зашифрованное сообщение	Клсфица

Вариант 7

Зашифрованное сообщение	Нцтэру

Вариант 8

Зашифрованное сообщение	Яукяэцм

Вариант 9

Зашифрованное сообщение	Фякъыоя

Вариант 10

Зашифрованное сообщение	цтплугн

Аффинный шифр

Афинный шифр – шифр простой замены, использующий в качестве ключа два числа. Эти числа (то есть ключ афинного шифра) определяют линейную зависимость порядковых номеров символов будущей шифровки от порядковых номеров заменямых символов открытой информации в используемом алфавите. Так например, если линейная зависимость афинного шифра $2x+8$, то символ «А» (порядковый номер символа равен 1) заменяется на «И» (порядковый номер символа равен 2*1+8=10).

Функция шифрования для каждой буквы:

$$E(x) = (ax - b) mod\ m, \quad (1)$$

где модуль m— размер алфавита,

пара a и b— ключ шифра.

Значение a должно быть выбрано таким, что a и m оказались взаимно простыми числами.

Функция расшифрования:

$$D(x) = a^{-1}(x - b) mod\ m, \quad (2)$$

где a^{-1} - обратное к a число по модулю m, то есть оно удовлетворяет уравнению

$$aa^{-1} mod\ m = 1. \quad (3)$$

Шифр был разработан в начале 20 века и использовался военными и правительственными организациями для передачи секретной информации.

Таблица 8. Алфавит для Аффинного шифра

№	Буква	№	Буква	№	Буква
1	А	12	К	23	Х
2	Б	13	Л	24	Ц
3	В	14	М	25	Ч
4	Г	15	Н	26	Ш
5	Д	16	О	27	Щ

Окончание табл. 8

№	Буква	№	Буква	№	Буква
6	Е	17	П	28	Ъ
7	Ё	18	Р	29	Ы
8	Ж	19	С	30	Ь
9	З	20	Т	31	Э
10	И	21	У	32	Ю
11	Й	22	Ф	33	Я

Таблица 9. Пример шифрования

Исходное сообщение	МИРЭА
Ключ	a=5, b=3
Зашифрованное сообщение	ВТЩШЖ

Исходное слово: МИРЭА

Решение:

Шифрование, с помощью функции E(x):

М -> E(x)=(ax+b) mod m = (5*14+3) mod 33=7 -> В;

И > E(x)=(ax+b) mod m = (5*10+3) mod 33=20 -> Т;

Р > E(x)=(ax+b) mod m = (5*18+3) mod 33=27 -> Щ;

Э > E(x)=(ax+b) mod m = (5*31+3) mod 33=26 -> Ш;

А > E(x)=(ax+b) mod m = (5*1+3) mod 33=8 -> Ж.

Дешифрование, с помощью функции D(x):

Так как $aa^{-1} \bmod m = 1$, то a-1 = 20 (5*20 mod 33=1)

В -> D(x)=a^{-1}(x-b) mod m = 20*(7-3) mod 33=14 -> М

Т > B(x)= a^{-1}(x-b) mod m = 20*(20-3) mod 33=20 -> И

И так далее.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	хжнпк
Ключ	a=5, b=3

Вариант 2

Зашифрованное сообщение	пичиы
Ключ	a=5, b=5

Вариант 3

Зашифрованное сообщение	кжзьж
Ключ	a=5, b=3

Вариант 4

Зашифрованное сообщение	йтдак
Ключ	a=5, b=7

Вариант 5

Зашифрованное сообщение	лрэрз
Ключ	a=5, b=4

Вариант 6

Зашифрованное сообщение	фають
Ключ	a=5, b=3

Вариант 7

Зашифрованное сообщение	ёпгпщ
Ключ	a=5, b=3

Вариант 8

Зашифрованное сообщение	циысз
Ключ	a=5, b=5

Вариант 9

Зашифрованное сообщение	срвлз
Ключ	a=5, b=4

Вариант 10

Зашифрованное сообщение	зиыех
Ключ	a=5, b=5

Двоичный код

Двоичное кодирование – это процесс преобразования информации в бинарный код, то есть в последовательность нулей и единиц. Это позволяет хранить информацию в виде двоичного кода, который может быть легко обработан компьютером. Двоичное кодирование используется во многих областях, таких как программирование, базы данных, криптография и другие. .

Каждый ноль или единица - это бит. А каждые 8 бит - это 1 байт. В одном бите, как правило, большое количество информации сохранить невозможно, но вот байт (8 бит) уже может нести в себе больше информации. Например, в виде последовательности байт можно представить:

1) просто число. Например, 00000001 - это число "1" записанное в двоичном виде. 00000010 - это двойка, 00000011 - это тройка и т.д;

2) можно сохранять текстовые данные. В этом случае каждое простое число из предыдущего шага по специальной таблице символов (например, ASCII) сопоставляется с буквой. Например, 01100001 = 97 = "a" (маленькая латинская буква а). 01100010 = 98 = "b" и так далее;

3) есть и более сложный вариант. Когда бинарные данные, состоящие из нулей и единиц обрабатываются специальным образом в зависимости от того, что это за файл. Примеры бинарных файлов: файл любой программы, файл архива, фотографии или mp3 трек. Кстати, файлы Microsoft Word тоже являются бинарными несмотря на то, что в них может храниться текстовая информация. Просто так их содержимое не просмотреть, и, как правило, в этом мало смысла,

т.к. "видимых" и понятных человеку символов там обычно очень мало. Вместо этого стоит поискать ту программу, которая сможет работать именно с этим типом файлов.

Например, используя алфавит, где а - 1, б -2 и т.д., можно сказать, что каждый символ будет весить 8 бит.

Таблица 10. Двоичный код для букв алфавита

№	Буква	Двоичный код	№	Буква	Двоичный код	№	Буква	Двоичный код
1	А	00000001	12	К	00001100	23	Х	00010111
2	Б	00000010	13	Л	00001101	24	Ц	00011000
3	В	00000011	14	М	00001110	25	Ч	00011001
4	Г	00000100	15	Н	00001111	26	Ш	00011010
5	Д	00000101	16	О	00010000	27	Щ	00011011
6	Е	00000110	17	П	00010001	28	Ъ	00011100
7	Ё	00000111	18	Р	00010010	29	Ы	00011101
8	Ж	00001000	19	С	00010011	30	Ь	00011110
9	З	00001001	20	Т	00010100	31	Э	00011111
10	И	00001010	21	У	00010101	32	Ю	00100000
11	Й	00001011	22	Ф	00010110	33	Я	00100001

Пример шифрования

Исходный текст: МИРЭА

Зашифрованное сообщение: 00001110 00001010 00010010 00011111 00000001

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	00001101 00000110 00001100 00011000 00001010 00100001
Ключ	см. табл. 10

Вариант 2

Зашифрованное сообщение	00010011 00010100 00010101 00000101 00000110 00001111 00010100
Ключ	см. табл. 10

Вариант 3

Зашифрованное сообщение	00011111 00001100 00001001 00000001 00001110 00000110 00001111
Ключ	см. табл. 10

Вариант 4

Зашифрованное сообщение	00001001 00000001 00011001 00000110 00010100
Ключ	см. табл. 10

Вариант 5

Зашифрованное сообщение	00010011 00000110 00010011 00010011 00001010 00100001
Ключ	см. табл. 10

Вариант 6

Зашифрованное сообщение	00010011 0010000 00010000 00000010 00011011 00000110 00001111 00001010 00000110
Ключ	см. табл. 10

Вариант 7

Зашифрованное сообщение	00010011 00001010 00001110 00000011 00010000 00001101
Ключ	см. табл. 10

Вариант 8

Зашифрованное сообщение	00001101 00010000 00000100 00001010 00001111
Ключ	см. табл. 10

Вариант 9

Зашифрованное сообщение	00010001 00000001 00010010 00010000 00001101 00011110
Ключ	см. табл. 10

Вариант 10

Зашифрованное сообщение	00000001 00010101 00010100 00000110 00001111 00010100 00001010 00010110 00001010 00001100 00000001 00011000 00001010 00100001
Ключ	см. табл. 10

Русская литорея

Литорея – это метод тайнописи, который заключается в замене букв на символы или слова. Шифр использовался для шифрования текстов в России в XV-XVII веках. Существует несколько видов литореи, включая простую литорею, сложную литорею и монокондическую литорею. Простая литорея заменяет каждую букву на символ, сложная литорея заменяет группы букв на слова, а монокондическая литорея использует специальные символы для обозначения букв.

Простая, иначе называемая тарабарской грамотой, — это замена одних согласных букв на другие. Самый простой способ заключается в следующем: поставив согласные буквы в два ряда, в порядке:

Таблица 11. Русская литорея

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Для шифрования и дешифрования используют верхние буквы вместо нижних и наоборот, причём гласные остаются без перемены. Так, например, *МИРЭА= РИМЭА* и т. п. В усложнённом варианте буквы в строках располагались в случайном порядке.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	Сетдиоппая ауцикомия
Ключ	см. табл. 11

Вариант 2

Зашифрованное сообщение	Топкмосьпая мащока
Ключ	см. табл. 11

Вариант 3

Зашифрованное сообщение	Келкошое фацапие
Ключ	см. табл. 11

Вариант 4

Зашифрованное сообщение	Фагёкпая леллия
Ключ	см. табл. 11

Вариант 5

Зашифрованное сообщение	Этфарепадиоппая леллия
Ключ	см. табл. 11

Вариант 6

Зашифрованное сообщение	Нматкигелтая мащока
Ключ	см. табл. 11

Вариант 7

Зашифрованное сообщение	Лацошое кошамибелкшо
Ключ	см. табл. 11

Вариант 8

Зашифрованное сообщение	Сащомакощпая мащока
Ключ	см. табл. 11

Вариант 9

Зашифрованное сообщение	шоеппая тазецма
Ключ	см. табл. 11

Вариант 10

Зашифрованное сообщение	Амжикетума лилкеры
Ключ	см. табл. 11

Диск Альберти

Ещё один значительный шаг вперед в криптографии сделал известный итальянский философ, живописец, архитектор Леон Альберти. Он предложил шифр, основанный на использовании шифровального диска, сам он называл его шифром, «достойным королей».

Устройство представляло собой пару дисков разного диаметра. Внешний неподвижный диск, разбивался на 24 сектора, в них были вписаны 20 букв расположенных в естественном порядке и 4 цифры (от 1 до 4). Внутренний подвижный диск также был разделен на 24 сектора, по его окружности были вписаны все буквы смешенного алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замену ее на

соответствующую (стоящей под ней) букву шифрованного текста. После шифрования нескольких слов диск сдвигался на один шаг. Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

Рисунок 8. Диск Альберти

Пример изображен на рис. 9. Имея два таких прибора, корреспонденты договаривались о первой индексной букве на подвижном диске. При шифровании сообщения индексная буква ставилась против любой буквы внешнего диска. Отправитель сообщения информировал корреспондента о таком положении диска, записывая эту букву внешнего диска в качестве первой буквы шифротекста.

Следующая буква открытого текста отыскивалась на внешнем диске и стоящая против нее буква являлась результатом её зашифровывания. После того как несколько букв были зашифрованы, положение индексной буквы менялось, о чем также сообщалось корреспонденту. Такой шифр получил название многоалфавитного шифра.

На рис. 10 изображен пример диска Альберти на русском языке, где индексная буква О (стоит напротив А внешнего круга).

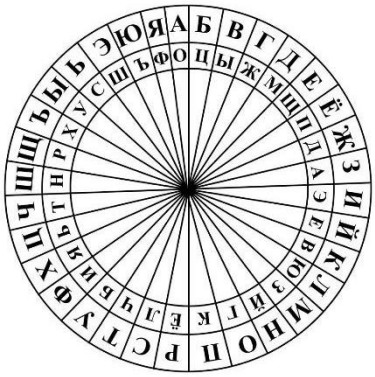

Рисунок 9. Диск Альберти с индексной буквой О

На рис. 10 изображено смещение внутреннего диска на 1 шаг влево после шифрования 5 символов.

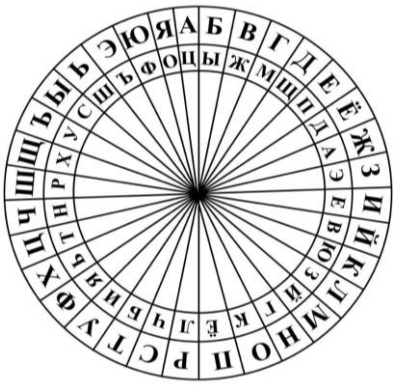

Рисунок 10. Диск Альберти после смещения

Пример

Исходное сообщение: РТУМИРЭА

Таблица 12. Пример шифрования

Индексная буква	5 символов по диску на рис. 9	3 символа по диску на рис. 10
Ц	ёчбзэ	лъц

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	ц ы е б и ч в д к и
Индексная буква	Диск на рис. 9

Вариант 2

Зашифрованное сообщение	ц б я ы т ы р ы е
Индексная буква	Диск на рис. 9

Вариант 3

Зашифрованное сообщение	ц а о ц о л б к ж ю
Ключ	Диск на рис. 9

Вариант 4

Зашифрованное сообщение	ц ё о м э г ж к з г
Ключ	Диск на рис. 9

Вариант 5

Зашифрованное сообщение	ц ц э ц ю э к б п ю
Ключ	Диск на рис. 9

Вариант 6

Зашифрованное сообщение	ц ц э ц ю э к б п ю
Ключ	Диск на рис. 9

Вариант 7

Зашифрованное сообщение	ц б б л ц ю т е к г
Ключ	Диск на рис. 9

Вариант 8

Зашифрованное сообщение	ж к з м к м л ц щ
Ключ	Диск на рис. 9

Вариант 9

Зашифрованное сообщение	ю к й й и б ц б
Ключ	Диск на рис. 9

Вариант 10

Зашифрованное сообщение	ю л к ю к щ е з
Ключ	Диск на рис. 9

Шифр Виженера

Шифр Виженера – это полиалфавитный шифр, который использует таблицу ключей для замены каждой буквы открытого текста на соответствующую букву зашифрованного текста. Таблица ключей состоит из последовательности алфавитов, и каждый алфавит используется для шифрования одного символа открытого текста.

Суть алгоритма шифрования проста. Шифр Виженера — это последовательность шифров Цезаря с различными значениями сдвига (ROTX — см. Шифр Цезаря). То есть к первой букве текста применяется преобразование, например, ROT5, ко второй, например, ROT17, и так далее. Последовательность применяемых преобразований определяется ключевой фразой, в которой каждая буква слова обозначает требуемый сдвиг, например, фраза ГДЕ ОН задает такую последовательность шифров Цезаря: ROT3-ROT4-ROT5-ROT15-ROT14, которая повторяется, пока не будет зашифрован весь текст сообщения. Так же используют таблицу Виженера.